

NIS2 Directive

Cheat sheet for the EU network and information security rules

Who it covers

- Medium and large organisations in the listed sectors: "essential" (large, Annex I) or "important" (Annex I medium, and Annex II).
- Some entities are covered whatever their size (public communications, trust services, DNS/TLD, central government).
- Each EU country writes NIS2 into its own law: check yours.

What you must do (Art. 21)

- Risk analysis and information security policies.
- Incident handling, business continuity and crisis management (backups, disaster recovery).
- Supply chain security: vet suppliers and set security terms.
- Secure acquisition, development and vulnerability handling.
- Cyber hygiene and training, cryptography, access control and multi-factor authentication.

Reporting a significant incident (Art. 23)

- Early warning: within 24 hours of becoming aware.
- Incident notification: within 72 hours.
- Final report: within one month of the incident notification.

Management is accountable (Art. 20)

- Management bodies must approve and oversee the measures, can be held responsible, and should be trained.

Penalties (Art. 34)

- Essential entities: up to EUR 10 million or 2% of worldwide turnover, whichever is higher.
- Important entities: up to EUR 7 million or 1.4%, whichever is higher.

First five actions

- 1. Work out whether you are in scope and which category. 2. Name an owner and brief management. 3. Run a risk assessment. 4. Write and test an incident plan with the 24/72-hour steps. 5. Review your key suppliers.